TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 01819/RPM

U.S. APPLICATION NO. (If known, see 37 CFR 1.5: 10/018605

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP 00/05642	19/JUNE/2000	25 JUNE 1999

TITLE OF INVENTION
SYSTEM FOR PROTECTED STORAGE AND MANAGEMENT IN A TTP SERVER

APPLICANT(S) FOR DO/EO/US: Marten DE BOER and Geert KLEINHUIS

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   - a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   - b. ☒ has been communicated by the International Bureau.
   - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   - a. ☐ is attached hereto.
   - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   - b. ☐ have been communicated by the International Bureau.
   - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:

Int. Search Report; Int'l. Preliminary Exam. Report; Dutch priority document w/translation; Request for Publn. of Assignment Infor; Change of Address Correspondence form; 3 sheets formal drawings (Figs. 1-3); Published Int'l. Appln. Pub. Pub. No. WO/01/01629A1; Forms PCT/ISA/220; PCT/IPEA/402; PCT/IPEA/401; PCT/IPEA/416; PCT/RO/101; PCT/RO/105

Express Mail Mailing Label No.: EV 0444 65569US

Date of Deposit: December 17, 2001

I hereby certify that this paper and any papers identified herein is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Angella Johnson

Angella Johnson

U.S. APPLICATION NO (if known, see 37 CFR 1.5) 10/018605	INTERNATIONAL APPLICATION NO PCT/EP 00/05642	ATTORNEY'S DOCKET NUMBER 01819/RPM

21.☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1040.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$890.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$740.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 890.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	9 - 20 =		x **$18.00**	$	
Independent claims	1 - 3 =		x **$84.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$280.00**	$	

TOTAL OF ABOVE CALCULATIONS =	$ 890.00	
□ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. ÷	$	
SUBTOTAL =	$ 890.00	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).	$	
TOTAL NATIONAL FEE =	$ 890.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$	
TOTAL FEES ENCLOSED =	$ 890.00	
	Amount to be refunded:	$
	charged:	$

a. ☒ A check in the amount of $ 890.00 to cover the above fees is enclosed.

b. □ Please charge my Deposit Account No. ______________ in the amount of $ __________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-1378. A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

FRISHAUF, HOLTZ, GOODMAN, LANGER & CHICK
767 Third Ave - 25th floor
New York, N.Y. 10017-2023

SIGNATURE

ROBERT P. MICHAL
NAME

35,614
REGISTRATION NUMBER

Dated: December 17, 2001

RPM/ajj

Attorney Docket No. 01819/RPM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Marten DE BOER et al
Serial No.	:	Based on PCT/EP00/05642
Filed	:	Herewith
For	:	SYSTEM FOR PROTECTED STORAGE AND MANAGEMENT IN A TTP SERVER
Art Unit	:	
Examiner	:	

Express Mail Mailing Label
No.: EV 0444 65569US
Date of Deposit: December 17, 2001
I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Angella Johnson
ANGELLA JOHNSON

In the event that this Paper is late filed, and the necessary petition for extension of time is not filed concurrently herewith, please consider this as a Petition for the requisite extension of time, and to the extent not tendered by check attached hereto, authorization to charge the extension fee, or any other fee required in connection with this Paper to Account No. 06-1378.

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents

SIR:

IN THE SPECIFICATION:

Page 1: Please insert the following as the first sentence:

--This application is a U.S. National Phase Application under 35 USC 371 of International Application PCT/EP 00/05642 (published in English) filed June 19, 2000.--

A marked-up copy of page 1 is attached hereto.

Respectfully submitted,

Robert P. Michal
Reg. No. 35,614

Frishauf, Holtz, Goodman, Langer & Chick, P.C.
767 Third Avenue - 25th Floor
New York, New York 10017-2023
Tel. No. (212) 319-4900
Fax Nos. (212) 319-5101
RPM:ajj

System for protected storage and management in a TTP server.

BACKGROUND OF THE INVENTION

The invention relates to a system for protected storage and management in a TTP server [TTP = Trusted Third Party] of copies of digital files transmitted, by way of a transmission channel, from a first to a second user.

The invention relates to, in other words, a timeless key and storage system for the benefit of the long-term storage of electronically exchanged (digitally protected) information and protectedly making available (secure retrieving) the stored data.

The few known systems have the following drawbacks:

1) Current protection techniques have a restricted hackability duration guarantee.

2) Limited protection guarantees prior to, during and after long-term storage.

3) Much storage space and effort are required for key management.

4) Protected long-term storage and the associated key and storage management is now either not regulated or very complex in setup.

5) Due to the ever changing software and hardware, it is very difficult to guarantee electronic timelessness.

B. SUMMARY OF THE INVENTION

The object of the invention is to overcome said drawbacks. For this purpose, the invention provides for a system having means for carrying out the functionalities: "Secure Archiving", "Re-encryption" and "Secure Retrieval", which will be discussed below. In this connection, the optional items "Digital Sign" and "Time Stamp" will be discussed separately.

"Secure Archiving"

If, according to the current state of the art, a file is transmitted from a first user to a second user in a safe way, the file is enciphered with a symmetrical session key, which in its turn is enciphered with the public key of the second user. Said second user may decipher the session key with his private key and decipher the file itself with the session key deciphered in this manner.

--This application is a U.S. National Phase Application under 35 USC 371 of International Application PCT/EP 00/05642 (published in English) filed June 19, 2000.--

System for protected storage and management in a TTP server.

BACKGROUND OF THE INVENTION

The invention relates to a system for protected storage and management in a TTP server [TTP = Trusted Third Party] of copies of digital files transmitted, by way of a transmission channel, from a first to a second user.

The invention relates to, in other words, a timeless key and storage system for the benefit of the long-term storage of electronically exchanged (digitally protected) information and protectedly making available (secure retrieving) the stored data.

The few known systems have the following drawbacks:

1) Current protection techniques have a restricted hackability duration guarantee.

2) Limited protection guarantees prior to, during and after long-term storage.

3) Much storage space and effort are required for key management.

4) Protected long-term storage and the associated key and storage management is now either not regulated or very complex in setup.

5) Due to the ever changing software and hardware, it is very difficult to guarantee electronic timelessness.

B. SUMMARY OF THE INVENTION

The object of the invention is to overcome said drawbacks. For this purpose, the invention provides for a system having means for carrying out the functionalities: "Secure Archiving", "Re-encryption" and "Secure Retrieval", which will be discussed below. In this connection, the optional items "Digital Sign" and "Time Stamp" will be discussed separately.

"Secure Archiving"

If, according to the current state of the art, a file is transmitted from a first user to a second user in a safe way, the file is enciphered with a symmetrical session key, which in its turn is enciphered with the public key of the second user. Said second user may decipher the session key with his private key and decipher the file itself with the session key deciphered in this manner.

According to the invention, the session key is also enciphered by the first user with the public key of an "in-line" TTP server (i.e., included in the transmission channel between the first and second users), which TTP server deciphers the session key received with his private key. Thereafter, the TTP server enciphers the deciphered session key with a "public" storage key. The session key enciphered with said public storage key and the file enciphered with the session key are subsequently stored in a storage medium of the TTP.

It should be noted that above and below there is spoken of public and private keys. These are generally known. In general, a public and a private key constitute an asymmetric pair of keys. If a file or a code is enciphered with the public key of an asymmetric pair of keys, said file or code may be deciphered only with the help of the associated private key and vice versa. In general, the public keys are available to "the public", e.g., by way of a publicly accessible data base, such as www.pgp.com. In the present application, it is assumed that the users and the TTP each dispose of a pair of keys, each consisting of a public and a private key, and in particular intented for protecting the mutual data exchange of the files and codes. In addition, the TTP disposes of a pair of keys which is used within the TTP only; the "public" and private keys serve as protected storage or recovery ("secure retrieval"), as the case may be, of files and codes. The public storage key is not, as is normally the case for public keys, put at the disposal of the public.

"Re-encryption"

By way of "periodic maintenance" - from security considerations - the TTP server may at regular points in time store the file once again in the storage medium. For this purpose, the session key with which the file was enciphered is first recovered by deciphering - with the private storage key - the stored (enciphered) session key. Subsequently, the enciphered file stored in the storage medium is deciphered with the recovered session key.

The TTP server then generates a new asymmetric pair of storage keys, consisting of a new public storage key (which is not made available outside the TTP) and a new private storage key, and a new version of the symmetrical session key, whereafter the TTP enciphers the deciphered file with the new session key and stores it in the storage medium.

The TTP also enciphers the new session key with the new public storage key and stores said enciphered session key in the storage medium.

"Secure Retrieval"

For protected recovery of the stored file, and transmission thereof to the first and/or second user, the symmetrical session key is recovered from the storage medium by deciphering, with the private storage key, the stored enciphered session key. The recovered session key is subsequently enciphered with the current public key of the first or second user, as the case may be, and transmitted to said user by way of the transmission channel, together with a copy of the file stored in the storage medium, enciphered with the session key. After having received the enciphered session key, the user may recover the session key therefrom by deciphering with his private key. Subsequently, the user may decipher the file enciphered with the session key using the recovered session key.

"Digital Sign"

The public key of the first user may - as is well-known - be used to verify a digital signature of the file. A problem arises if - which frequently occurs - the first user at a certain point in time, after the file has been stored in the TTP server, generates a new pair of keys (comprising a public and a private key) and discontinues the old one. For this reason, it is of importance to store the (original) public key of the first user in the TTP server, since only said original key may be used for verifying the digital signature of the stored, later retrievable file.

For this case, the TTP server, after having received the enciphered file, also enciphers the - at that point in time publicly available - public key of the first user, with the public storage key, and stores said enciphered public key in the storage medium.

Periodically, the TTP server -- as "periodical maintenance" -- deciphers the enciphered (original) public key, stored in the storage medium, of the first user having the private storage key, and enciphers the deciphered public key of the first user having the newly generated public storage key, and stores said freshly enciphered key in the storage medium.

The public key of the first user may — upon retrieving the stored file — be recovered from the storage medium by deciphering, with the private storage key, said stored key. The public key of the first user recovered in this manner is subsequently enciphered with the — at that point in time publicly available — public key of the retrieving first or second user, and transmitted by way of the transmission channel. After having received said enciphered public key, the user may recover the original public key of the first user by deciphering his current private key; subsequently, the digital signature of the recovered file may be verified using the recovered original public key of the first user.

"Time Stamp"

If so desired, the TTP server, after the enciphered file has been received and stored, may generate a time stamp and store it, linked to the stored file and enciphered with the public storage key, in the storage medium. In the event of retrieving the stored file by the first or second user, the time stamp is deciphered and subsequently enciphered with the public key valid for said user and transmitted to the user. The user may decipher the enciphered time stamp with his current private key.

DESCRIPTION OF THE FIGURES

Below, the invention is illustrated in further detail by reference to several figures. Figures 1, 2 and 3 illustrate the functions "Secure Archiving", "Re-encryption" and "Secure Retrieval", including the items "Digital Sign" and the "Time Stamp".

FIG. 1: "Secure Archiving"

A file **Txt** is transmitted from a first user **A** to a second user **B** after having been enciphered with a symmetical session key **SesKey**. Said session key is enciphered with the public key **PubKeyB** of the second user. The latter may decipher the session key with his private key **SecKeyB** and the file itself with the deciphered session key.

The session key is also enciphered by the first user with the public key of the TTP server **PubKeyTTP**, which, after having received it, deciphers said session key with his private key **SecKeyTTP**. Thereafter the TTP server enciphers the deciphered session key with a "public" storage key **PubStorKey** of the TTP.

The (transmission) keys of the users A and B each form an asymmetrical pair of keys, **KeyPairA** and **KeyPairB**, respectively, consisting of **PubKeyA** and **SecKeyA**, and **PubKeyB** and **SecKeyB**, respectively. The TTP uses the pair of keys **KeyPairTTP**, consisting of **PubKeyTTP** and **SecKeyTTP**. Finally, for the protected storage of an asymmetrical pair of keys **StorKeyPair**, consisting of the keys **PubStorKey** and **SecStorKey**; contrary to the preceding public keys, **PubStorKey** nor **SecStorKey** is publicly available, but is used exclusively within the TTP.

The session key **(SesKey)PubStorKey** enciphered with the public storage key **PubStorKey** and the file **(Txt)SesKey** enciphered with the session key **SesKey** are subsequently stored in the storage medium **DB** of the TTP.

"Digital Sign"

The public key **PubKeyA** of the first user **A** may be used to verify a digital signature **DigSign** of the file **Txt**. In this case, the TTP server, after having received the enciphered file **(Txt)SesKey**, also enciphers the - at that point in time publicly available - public key **PubKeyA** from the first user **A**, with the public storage key **PubStorKey**, and stores said enciphered public key **(PubKeyA)PubStorKey** in the storage medium **DB**.

"Time Stamp"

After having received and stored the enciphered file **(Txt)SesKey**, the TTP server may generate a time stamp **TStamp** and store it, after enciphering with the public storage key **PubStorKey** and linked to the stored file, in the storage medium **DB** as **(TStamp)PubStorKey**.

FIG. 2: "Re-encryption"

As "periodical maintenance", the TTP server deciphers the enciphered file **(Txt)SesKey** stored in the storage medium with the session key **SesKey**, which for that purpose is recovered by deciphering the stored session key **(SesKey)PubStorKey** with the private storage key **SecStorKey**. The TTP server subsequently generates a fresh pair of storage keys **StorKeyPair**, comprising a new "public" storage key **PubStorKey'** and a new private storage key **SecStorKey'**, as well as a new version of the symmetrical session key **SesKey'**. The TTP subsequently enciphers the deciphered file **Txt** with the new session key **SesKey'** and stores the file **(Txt)SesKey'** enciphered in this manner in the storage medium **DB**.

The TTP also enciphers the new session key with the new public storage key **PubStorKey'** and stores the session key **(SesKey')PubStorKey'** enciphered in this manner in the storage medium **DB**.

"Digital Sign"

During the periodical maintenance, the TTP server also deciphers the enciphered public key **(PubKeyA)PubStorKey** stored in the storage medium of the first user with the private storage key **SecStorKey**, and subsequently enciphers the deciphered public key **PubKeyA** with the newly generated public storage key **PubStorKey'** and stores the public key **(PubKeyA)PubStorKey'** enciphered in this manner in the storage medium.

"Time Stamp"

During the periodical maintenance, the TTP server also deciphers the enciphered time stamp **(TStamp)PubStorKey** stored in the storage medium with the private storage key **SecStorKey**, and subsequently enciphers the deciphered time stamp with the newly generated public storage key **PubStorKey'** and stores the time stamp **(TStamp)PubStorKey'** enciphered in this manner in the storage medium.

FIG. 3: "Secure Retrieval"

For protected recovery of the file **Txt**, and the transmission thereof to the first and second users **A** and **B**, respectively, the symmetrical session key **SesKey** is recovered from the storage medium by deciphering, with the private storage key **SecStorKey**, the stored enciphered session key **(SesKey)PubStorKey**. The recovered session key **SesKey** is subsequently enciphered with the then current public key **PubKeyA`** or **PubKeyB`**, as the case may be, from the querying first or second user **A** or **B**, as the case may be, and transmitted to said user by way of the transmission channel, together with a copy of the file stored in the storage medium, with the user, after having received the enciphered session key **(SesKey)PubKeyA˜** or **(SesKey)PubKeyB˜**, being capable of recovering the session key therefrom by deciphering, with his private key **SecKeyA˜** or **SecKeyB˜**, as the case may be, and subsequently being capable of deciphering the file **(Txt)SesKey** using the recovered session key.

"Digital Sign"

The original public key **PubKeyA** of the first user, necessary for verifying the digital signature of the recovered file, may be recovered from the storage medium by deciphering, with the private storage key **SecStorKey**, the stored public key **(PubKeyA)PubStorKey** of the first user enciphered with the public storage key. The deciphered public key **PubKeyA** of the first user recovered in this manner is subsequently enciphered with the current public key **PubKeyA˜** or **PubKeyB˜**, as the case may be, of the retrieving first or second user **A** or **B**, as the case may be, and transmitted to the user by way of the transmission channel. After having received said enciphered public key **(PubKeyA)PubKeyA˜** or **(PubKeyA)PubKeyB˜**, as the case may be, the user may recover the original public key **PubKeyA** of the first user therefrom by deciphering, with his current private key **SecKeyA˜** or **SecKeyB˜**, as the case may be. Subsequently, the digital signature **DigSign** of the file **Txt** may be verified using the recovered public key **PubKeyA** of the first user.

It should be noted that it is preferable to - otherwise than is shown in FIG. 3 - not transmit the digital signature **DigSign** unencipheredly to the first or second user, as the case may be, but enciphered with the public key of user **A** or **B**, as the case may be: instead of **"DigSign"**, the TTP server then transmits **"(DigSign)PubKeyA˜"** or **"(DigSign)PubKeyB˜"**, as the case may be. At the user's side, the digital signature may be recovered by deciphering, with the private keys of **A** and **B**, **SecKeyA** and **SecKeyB**, respectively.

"Time Stamp"

When the stored file is retrieved by the first or second user, the time stamp is first retrieved by deciphering

(TStamp)PubStorKey with the private storage key **SecStorKey**. The recovered time stamp is subsequently enciphered with the user's current public key **PubKeyA'** or **PubKeyB'**, as the case may be, and transmitted to said user. Thereafter, the user may decipher the enciphered time stamp **(TStamp)PubKeyA'** or **(TStamp)PubKeyB'**, as the case may be, with his current private key **SecKeyA'** or **SecKeyB'**, as the case may be.

CLAIMS

1. System for protectedly storing and managing, in a TTP server, copies of digital files which are transmitted, by way of a transmission channel, from a first to a second user, characterised in that

- a file (Txt) is transmitted from the first user (A) to a second user (B) after having been enciphered with a symmetrical session key (SesKey), which session key is enciphered using the public key (PubKeyB) of a first asymmetrical pair of keys (KeyPairB) associated with the second user, which second user, after having received it, may decipher the session key using the private key (SecKeyB) of said first asymmetrical pair of keys (KeyPairB) and subsequently may decipher the file using the session key deciphered in this manner, the session key (SesKey) also being enciphered by the first user (A) using the public key (PubKeyTTP) of a second asymmetrical pair of keys (KeyPairTTP) associated with the TTP server, which TTP server, after having received it, deciphers said session key using the private key (SecKeyTTP) from said second asymmetrical pair of keys (KeyPairTTP), whereafter the TTP server enciphers the deciphered session key (SesKey) using the public key of a third asymmetrical pair of keys (StorKeyPair), hereinafter to be referred to as public storage key (PubStorKey), and stores the session key ((SesKey)PubStorKey) enciphered with said storage key, together with the file ((Txt)SesKey) enciphered with the session key (SesKey), in a storage medium (DB).

2. System according to claim 1, characterised in that, periodically,

- the TTP server deciphers the enciphered file ((Txt)SesKey) stored in the storage medium with the session key (SesKey), which for that purpose is recovered in advance by deciphering the stored enciphered session key ((SesKey)PubStorKey) with the private key of the third pair of keys (StorKeyPair), hereinafter to be referred to as the private storage key (SecStorKey);

- the TTP server subsequently generates a new version of the third pair of keys, comprising a new public storage key (PubStorKey') and a new private storage key (SecStorKey'), and a new version of the symmetrical session key (SesKey'), whereafter the TTP enciphers the deciphered file (Txt) with the new session key (SesKey') and stores the file ((Txt)SesKey') enciphered in this manner in the storage medium (DB);
- the TTP server enciphers the new session key (SesKey') with the new public storage key (PubStorKey') and stores the session key ((SesKey')PubStorKey') enciphered in this manner in the storage medium (DB).

3. System according to claim 1, characterised in that, for protected recovery of the file (Txt) and transmission thereof to the first user (A) or the second user (B), as the case may be, the symmetrical session key (SesKey) is recovered from the storage medium by deciphering, with the private storage key (SecStorKey), the stored enciphered session key ((SesKey)PubStorKey), whereafter the recovered session key (SesKey) is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to the user by way of the transmission channel, together with a copy of the file ((Txt)SesKey) stored in the storage medium, with the user, after having received the enciphered session key ((SesKey)PubKeyA' or (SesKey)PubKeyB', as the case may be), being capable of recovering the session key therefrom by deciphering using the user's private key (SecKeyA' or SecKeyB', as the case may be), and subsequently being capable of deciphering the enciphered file ((Txt)SesKey) using the recovered session key.

4. System according to claim 1, the public key (PubKeyA) of the first user (A) being used to verify a digital signature (DigSign) of the file (Txt), characterised in that the TTP server, after having received the enciphered file ((Txt)SesKey), also enciphers the then current public key (PubKeyA) of the first user (A) using the public storage key (PubStorKey), and stores said enciphered public key ((PubKeyA)PubStorKey) in the storage medium (DB).

5. System according to claim 4, characterised in that, periodically,

- the TTP server deciphers the enciphered public key (PubKeyA) of the first user stored in the storage medium with the private storage key (SecStorKey);
- the TTP server subsequently generates a new version of the third pair of keys, comprising a new public storage key (PubStorKey') and a new private storage key (SecStorKey');
- the TTP server enciphers the deciphered public key (PubKeyA) of the first user with the new public storage key (PubStorKey') and stores said public key ((PubKeyA)PubStorKey'), enciphered in this manner, in the storage medium.

6. System according to claim 4, characterised in that the public key (PubKeyA) of the first user is recovered from the storage medium by deciphering, with the private storage key (SecStorKey), the stored enciphered public key ((PubKeyA)PubStorKey) of the first user,
that said original public key (PubKeyA) recovered in this manner is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted by way of the transmission channel to the first or second user, as the case may be, with the user, after having received said enciphered public key ((PubKeyA)PubKeyA' or (PubKeyA)PubKeyB', as the case may be) being capable of recovering the original public key (PubKeyA) of the first user therefrom by deciphering with his current private key (SecKeyA' or SecKeyB', as the case may be), and subsequently being capable of verifying the digital signature (DigSign) of the file (Txt) using the original public key (PubKeyA) of the first user recovered in this manner.

7. System according to claim 6, characterised in that the digital signature (DigSign) is enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to said first or second user, as the case may be, whereafter the receiving user recovers the digital signature by deciphering the

received, enciphered digital signature ((DigSign)PubKeyA' or (DigSign)PubKeyB', as the case may be) with his private key (SecKeyA' or SecKeyB', as the case may be).

8. System according to claim 1, characterised in that the TTP server, after having received the enciphered file ((Txt)SesKey) generates a time stamp (TStamp) and stores it, linked to the stored file and enciphered with the public storage key (PubStorKey), in the storage medium (DB).

9. System according to claim 8, characterised in that, in the event of retrieving the stored file by the first or second user (A or B, as the case may be) the enciphered time stamp ((TStamp)PubStorKey) is recovered by deciphering with the private storage key (SecStorKey), the recovered time stamp is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) for the querying user, and is transmitted to said user, whereafter the user may decipher the enciphered time stamp ((TStamp)PubKeyA' or (TStamp)PubKeyB', as the case may be) with the private key (SecKeyA' or SecKeyB', as the case may be) current for said user.

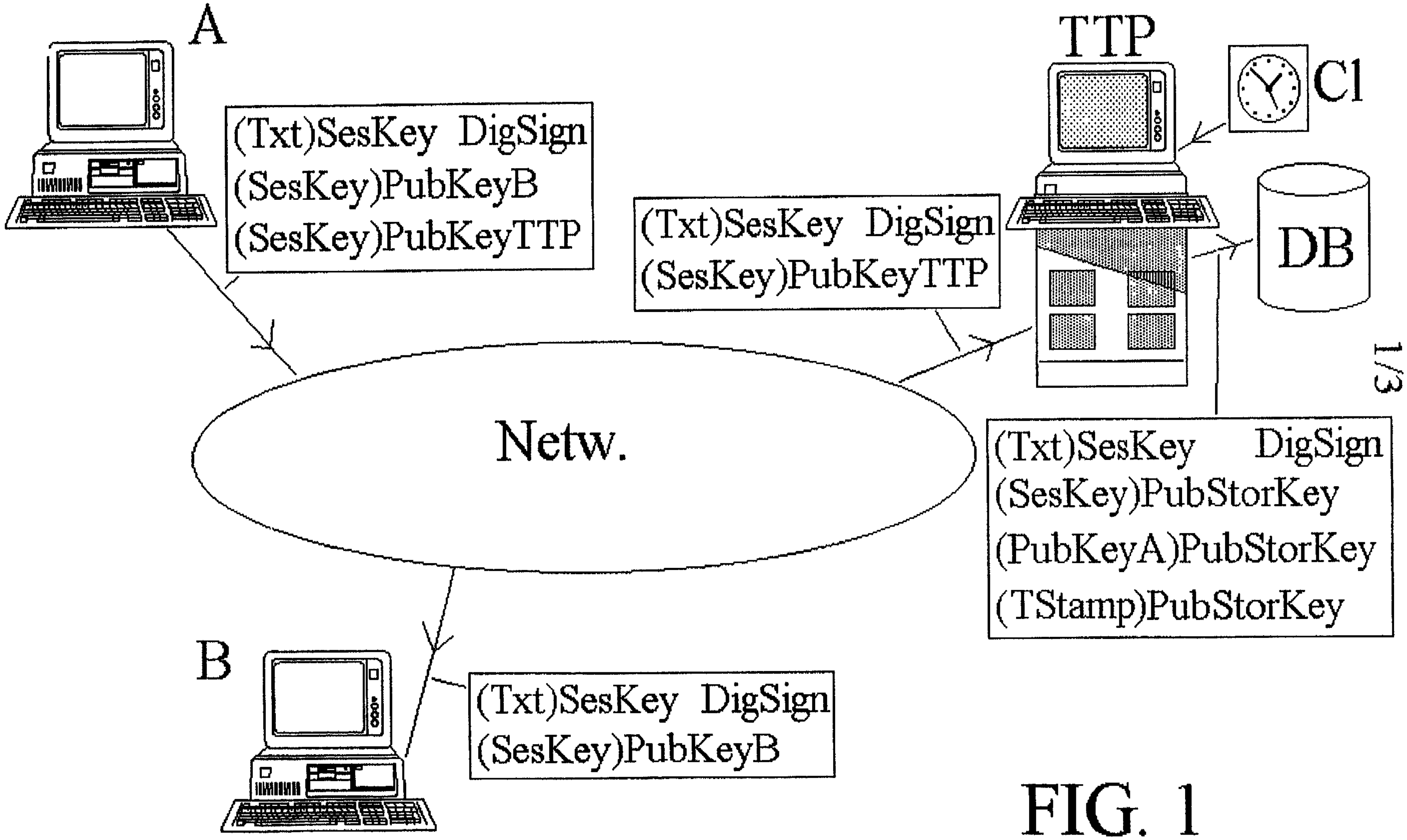
A
(Txt)SesKey DigSign
(SesKey)PubKeyB
(SesKey)PubKeyTTP
TTP
Cl
DB
(Txt)SesKey DigSign
(SesKey)PubKeyTTP
Netw.
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
B
(Txt)SesKey DigSign
(SesKey)PubKeyB

FIG. 1

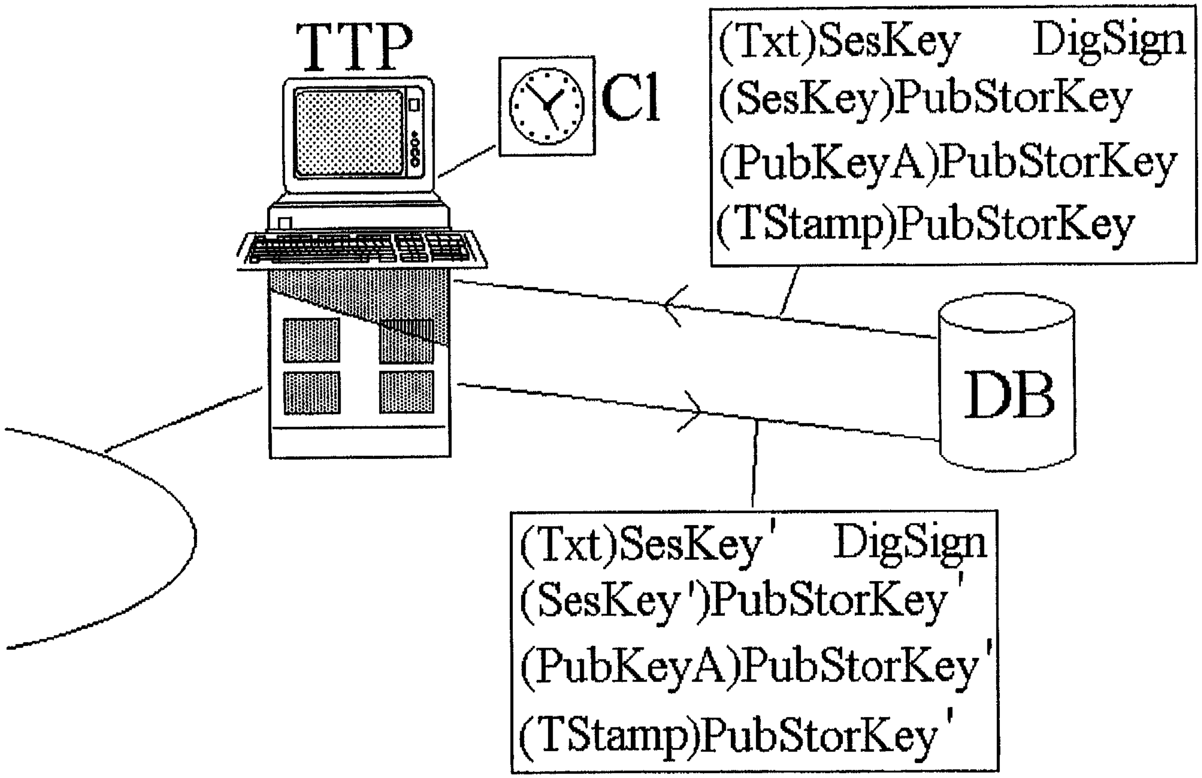
TTP
Cl
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
DB
(Txt)SesKey' DigSign
(SesKey')PubStorKey'
(PubKeyA)PubStorKey'
(TStamp)PubStorKey'

FIG. 2

3/3

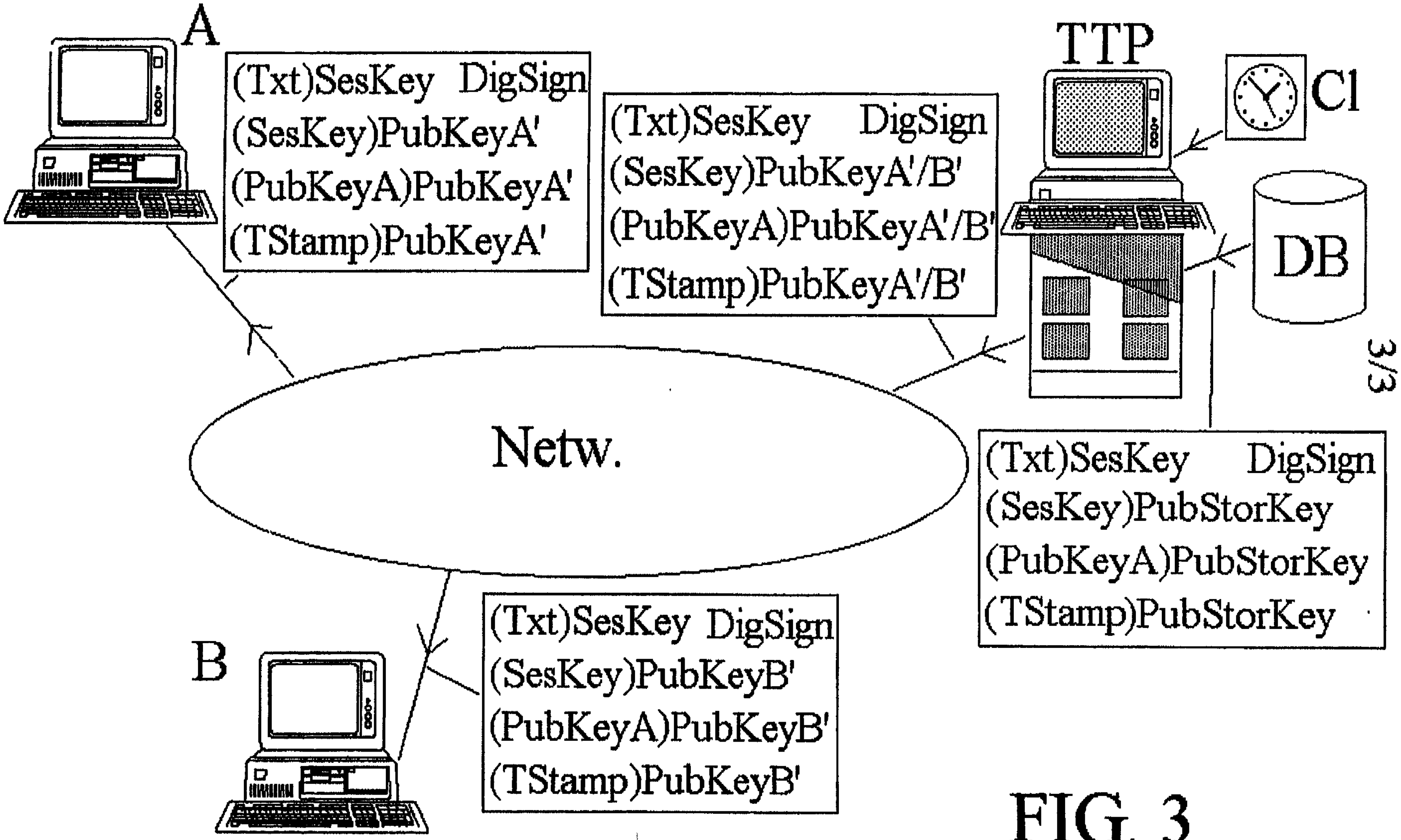
A
(Txt)SesKey DigSign
(SesKey)PubKeyA'
(PubKeyA)PubKeyA'
(TStamp)PubKeyA'
(Txt)SesKey DigSign
(SesKey)PubKeyA'/B'
(PubKeyA)PubKeyA'/B'
(TStamp)PubKeyA'/B'
TTP
Cl
DB
Netw.
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
B
(Txt)SesKey DigSign
(SesKey)PubKeyB'
(PubKeyA)PubKeyB'
(TStamp)PubKeyB'

FIG. 3

9/97FHGL&C

U.S. Attorney Docket ____________

APPLICATION FOR UNITED STATES LETTERS PATENT

PCT Declaration and Power of Attorney (35 U.S.C. 371(c)(4))
PCT Application - United States Designated Office

As a below named inventor, I declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

"System for protected storage and management in a TTP server"

described and claimed in International Application number PCT/EP00/05642 filed on June 19, 2000
and, if it was amended

I have reviewed and understand the contents of said specification, including claims.
I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I claim priority benefits under 35 USC §119 of: (i) any foreign application(s) for patent or inventor's certificate listed below; or (ii) any United States provisional application(s) listed below; and have also identified below any foreign application(s) for patent or inventor's certificate, or PCT international application having a filing date before that of the application(s) on which priority is claimed.

COUNTRY	APPLICATION NUMBER	DATE (day, month, year)	PRIORITY CLAIMED
NL	1012435	25 June 1999	Yes X No
			Yes No

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I appoint the following attorneys to prosecute this application and to transact all business in the U.S. Patent & Trademark Office connected therewith: Stephen H. Frishauf, Reg. No. 16,233; Leonard Holtz, Reg. No. 22,974; Herbert Goodman, Reg. No. 17,081; Thomas Langer, Reg. No. 27,264; Marshall J. Chick, Reg. No. 26,853; Richard S. Barth, Reg. No. 28,180; Douglas Holtz, Reg. No. 33,902; and Robert P. Michal, Reg. No. 35,614.

CORRESPONDENCE AND CALLS TO:

FRISHAUF, HOLTZ, GOODMAN, LANGER & CHICK, P.C.
767 Third Avenue - 25th Floor
New York, New York 10017-2023
Tel.: (212) 319-4900
Fax.: (212) 319-5101

INVENTOR: SIGNATURE	DATE	RESIDENCE AND POST OFFICE ADDRESS
Sign:	Date: 19-12-2001	Residence: (City & Country) Egypte 2, 9285 WX BUITENPOST The Netherlands NLX Post Office Address: P.O. Box 95321,2509 CH THE HAGUE, The Netherlands
100 Type: DE BOER Marten	Citizen of: The Netherlands	
Sign:	Date: 12-12-2001	Residence: (City & Country) Mindertfaen 1, 9264 TX EERNWOUDE The Netherlands NLX Post Office Address: P.O Box 95321, 2509 CH THE HAGUE, The Netherlands
200 Type: KLEINHUIS Geert	Citizen of: The Netherlands	